(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2002 (28.11.2002)

PCT

(10) International Publication Number
WO 02/095552 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/15466

(22) International Filing Date: 17 May 2002 (17.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/291,900 18 May 2001 (18.05.2001) US

(71) Applicant: **IMPRIVATA, INC.** [US/US]; 10 Maguire Road, Lexington, MA 02421 (US).

(72) Inventor: **TING, David, M., T.**; 27 Woodland Road, Sudbury, MA 01776 (US).

(74) Agent: **MIRANDA, David, G.**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/095552 A2

(54) Title: AUTHENTICATION WITH VARIABLE BIOMETRIC TEMPLATES

(57) Abstract: The invention relates to systems and methods for using a template in the authentication process using biometric data. In one embodiment, a module modifies a template of the reference set of biometric data with the candidate set of biometric data when the user is authenticated. In another embodiment, a module modifies a copy of the template of the reference biometric data with modification data thereby creating a challenge template. The client compares the challenge template to a candidate set of biometric data thereby creating a response vector. A module authenticates the user based on the response vector and the modification data.

Authentication With Variable Biometric Templates

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of and priority to the co-pending U.S. Provisional Application, Serial No. 60/291,900, filed May 18, 2001, entitled "Network-Based Biometric Authentication," the entirety of which is incorporated herein by reference.

FIELD OF INVENTION

[0002] The invention relates generally to biometrics. More specifically, in one embodiment, the invention relates to systems and methods for using biometric authentication over a network.

BACKGROUND

[0003] The Internet accords a global community of computer users access to applications and information that traditionally were highly restricted. For example, users can now undertake a wide variety of financial transactions online, or obtain access to financial and other sensitive records online. The increased accessibility of such information, while enormously convenient, jeopardizes privacy and invites tampering and electronic theft. In some known prior art systems, sensitive information that was once physically guarded can now be obtained on the Internet by anyone who can generate the correct server URL, logon and password.

[0004] Indeed, the mere need for Internet users to keep track of multiple URLs, logon names, passwords and PINs in order to access different information further increases the chances of unauthorized use and loss of private information. Users may resort to using the same logon name and password combinations for all accounts, rendering them equally vulnerable if unauthorized access to a single account is obtained. On the other hand, security-conscious users who maintain different logon names and passwords for individual accounts may, to avoid confusion, write them down where they may be found or store them on easily stolen devices such

as personal digital assistants—thereby undermining their own efforts. It can be argued that those who routinely change their passwords but record them on paper or in a computer file are at greater risk of being compromised than those who use a single but difficult-to-crack password. At the very least, such security-conscious individuals risk forgetting their access information, necessitating time-consuming calls to customer-support lines.

[0005] From the perspective of authentication, passwords and PINs cannot guarantee identity; the identification is no more reliable than the security of the password. In some known prior art systems with password authentication, the server carrying out a transaction can only prove that the correct password was entered—not that it was entered by an authorized person. A password can originate from password-cracking software just as easily as from the real user. Digital certificates improve security by authenticating an end point (i.e., that a message originated with a particular client terminal), but cannot create a non-repudiated link to support the claim that a particular user really did engage in a transaction.

SUMMARY OF THE INVENTION

[0006] The present invention utilizes biometric indicia to offer highly reliable authentication that creates links that cannot be repudiated for transactions initiated within the context of an authenticated session. Unlike passwords, which are no more than secrets vulnerable to theft, biometrics validation matches physical characteristics of the user against stored characteristics to identify the user. Once a user is positively identified, in one embodiment, the server unlocks and validates the user's credentials for presentation to other servers that request such authentication. A user's credentials may, for example, represent an account login/password combination or X.509 certificate. This biometric approach offers substantial flexibility in terms of accessibility (from computers, mobile devices, etc.) and relieves the user from responsibility for managing the integrity of such credentials. Biometric scanners are inexpensive and small, and may, for example, be easily incorporated into keyboards and mobile client devices.

[0007] In one embodiment, the authentication process can use an adaptive learning algorithm to improve the accuracy and reliability of matching a candidate set of biometric data against a user's biometrics profile (e.g., a reference set of biometric data stored as, for example, a template). Candidate sets of biometric data that result in successful matches are used to augment the profile and improve the statistics need to establish a subsequent reliable match. Upon authentication, new biometric data are introduced into the reference set associated with the profile if it is dissimilar or covers different portions of the biometrics (e.g., different areas of a finger) than other biometric data in the profile (e.g., template). The end result of this process is a gradual tuning of the matching process to the peculiarities exhibited by a user, thereby enhancing accuracy, speed and flexibility. This adaptation also accommodates the gradual changes in a subscriber's biometric data (e.g., fingerprints) over time.

[0008] In another embodiment, the authentication process uses a challenge-response protocol. Using of the challenge-response protocol, neither the server nor the client transmit a full set of biometric data across the network during the authentication session. The server makes a copy of the user's biometric data and modifies the copy to generate a challenge template. The modifying can include eliminating some of the geometric data representing the biometric features (e.g., only including the x, y coordinates of a feature) and inserting fictitious data (e.g., random noise). The server transmits the challenge template to the client. The client receives the challenge template and compares the challenge template to a candidate set of biometric data. Based on the comparison, the client generates a response vector. The response vector can be, for example, a hash code. The client transmits the response vector back to the server. The response vector indicates the portions of the challenge template that did not match the candidate set of biometric data. The server, knowing what fictitious data was inserted into the challenge template can determine if the mismatches sufficiently match the fictitious data. If they do, the server can authenticate the user.

[0009] In one aspect, the invention relates to a method for authentication using biometrics. The method comprises receiving a request for authentication of a user and receiving a first set of biometric data from the user. The method also comprises comparing the first set of biometric data with a second set of biometric data in storage; and modifying the second set of biometric data in storage based at least in part on the first set of biometric data, if the second set of biometric data sufficiently matches the first set of biometric data. In one embodiment, the method further includes replacing the second set of biometric data in storage with the first set of biometric data, if the second set of biometric data sufficiently matches the first set of biometric data.

[0010] In another embodiment, the method further includes identifying one or more features in the first set of biometric data, matching at least a portion of the one or more features in the second set of biometric data and augmenting the second set of biometric data with the first set of biometric data based at least in part on the matched features. In another embodiment, the method further includes augmenting the second set of biometric data with features from the first set of biometric data not presently included in the second set of biometric data. In still another embodiment, the method further includes augmenting statistical data associated with the second set of biometric data based at least in part on the first set of biometric data. In yet another embodiment, the method further includes augmenting statistical by increasing the weighting of the matched features.

[0011] In another embodiment, the method further includes normalizing and/or filtering the first set of biometric data. In another embodiment, the method further includes extracting from the first set of biometric data identifying features. The second set of biometric data may be stored in a supertemplate.

[0012] In another aspect, the invention relates to a system for authentication using biometrics. The system preferably comprises a network interface, a storage module, an authentication

module and an augmentor module. The network interface module may be configured to receive an authentication request requesting authentication of a user and to receive a first set of biometric data from the user. The storage module may be configured to store a second set of biometric data. In general, the authentication module is configured to compare the first set of biometric data with the second set of biometric data in storage. The augmentor module may modify the second set of biometric data in storage based at least in part on the first set of biometric data if the second set of biometric data sufficiently matches the first set of biometric data.

[0013] In one embodiment, the augmentor module is further configured to replace the second set of biometric data in storage with the first set of biometric data if the second set of biometric data sufficiently matches the first set of biometric data. In another embodiment, the augmentor module is further configured i) to identify one or more features in the first set of biometric data, ii) to match at least a portion of the one or more features in the second set of biometric data and iii) to augment the second set of biometric data with the first set of biometric data based at least in part on the matched features. In still another embodiment, the augmentor module is further configured to augment the second set of biometric data with features from the first set of biometric data not presently included in the second set of biometric data.

[0014] In another embodiment, the augmentor module is further configured to augment statistical data associated with the second set of biometric data based at least in part on the first set of biometric data. For example, the augmentor module may be configured to increase the weighting of the matched features. In another embodiment, the system further comprises a normalizer module configured to normalize the first set of biometric data. In still another embodiment, the system further comprises a filter module configured to filter the first set of biometric data. In yet another embodiment, the system further comprises an extractor module configured to extract identifying features from the first set of biometric data. The second set of biometric data may be stored in a supertemplate.

[0015] In another aspect, the invention relates to an article of manufacture having computer-readable program portions embodied therein for authentication using biometrics. The article comprises computer-readable program portions for performing the method steps as described above.

[0016] In one aspect, the invention relates to a method for authentication using biometrics. The method comprises providing a reference template with a reference set of biometric data associated with an individual and receiving an authentication request associated with a user. The method also comprises generating a copy of the reference template and modifying the copy of the reference template with modification data to generate a challenge template. In general, the method also comprises transmitting the challenge template, receiving a response vector based at least in part on the challenge template and a candidate set of biometric data, and authenticating the user as the individual associated with the reference set of biometric data based at least in part on the response vector and the modification data. In one embodiment, the method further includes receiving the candidate set of biometric data associated with the user and comparing the candidate set of biometric data with the challenge template in order to generate the response vector.

[0017] In another embodiment, the method further includes determining features in the candidate set of biometric data that match, and determining features in the candidate set of biometric data that do not match. The user may be authenticated as the individual associated with the reference set of biometric data if the degree of feature matching is not less than a predetermined threshold and the mismatched features sufficiently match the modification data.

[0018] In another embodiment, the method further includes registering the individual by generating the reference template with the reference set of biometric data from the individual. In yet another embodiment, the method further includes authenticating the user as the individual associated with the reference set of biometric data if at least a portion of the data represented by

the response vector sufficiently matches the modification data. The modification data may contain, for example, random data. The response vector may be a hash result. In some embodiments, the reference template is a portion of a supertemplate.

[0019] In another aspect, the invention relates to a system for authentication using biometrics. The system preferably includes a reference template, a modification module and an authentication module. In general, the reference template has a reference set of biometric data associated with an individual. The modification module is preferably configured to generate a copy of the reference template and to modify the copy of the reference template with modification data to generate a challenge template. The authentication module may be configured i) to receive a response vector based at least in part on the challenge template and a candidate set of biometric data and ii) to authenticate a user as the registered individual in response to the response vector and the modification data.

[0020] In one embodiment, the system further comprises a client in communication with the server. The client preferably includes a comparator module configured to compare the candidate set of biometric data, associated with the user, with the challenge template in order to generate the response vector. In another embodiment, the comparator module is further configured i) to determine features in the candidate set of biometric data that match and ii) to determine features in the candidate set of biometric data that do not match.

[0021] The authentication module may authenticate the user as the individual associated with the reference set of biometric data if the degree of feature matching is not less than a predetermined threshold and the mismatched features sufficiently match the modification data. The system may comprise a registration module configured to generate the reference template with the reference set of biometric data from the individual. The authentication module may be further configured to authenticate the user as the individual associated with the reference set of biometric data if at

least a portion of the data represented by the response vector sufficiently matches the modification data.

[0022] In another aspect, the invention relates to an article of manufacture having computer-readable program portions embodied therein for authentication using biometrics. The article comprises computer-readable program portions for performing the method steps described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The above and further advantages of the invention may be better understood by referring to the following description taken in conjunction with the accompanying drawing, in which:

[0024] FIG. 1 is block diagrams of illustrative embodiments of a system to authenticate a user using augmented biometric data accordance with the invention;

[0025] FIG. 2 is a block diagram of an illustrative embodiment of a supertemplate used to authenticate a user in accordance with the invention;

[0026] FIG. 3 is a block diagram of another illustrative embodiment of a system to authenticate a user using augmented biometrics in accordance with the invention;

[0027] FIG. 4 is a block diagram of another illustrative embodiment of a supertemplate used to authenticate a user in accordance with the invention; and

[0028] FIG. 5 is a flow diagram of an illustrative embodiment of a process to authenticate a user using augmented biometrics in accordance with the invention.

DETAILED DESCRIPTION

[0029] In broad overview, FIG. 1 illustrates an embodiment of a system 100 to authenticate a user using augmented biometric data in accordance with the invention. The system 100 includes a first computing system ("a server node") 108 and a second computing system ("a client node")

112, all in communication with a network 116. The server node 108 and the client node 112 are in communication with the network using communication channels 120.

[0030] For example, the network 116 and the communication channels 120 can be part of a local-area network (LAN), such as a company Intranet, a wide area network (WAN) such as the Internet or the World Wide Web or the like. The nodes 108 and 112 communicate with the network 116 through the communication channels 120 using any of a variety of connections including, for example, standard telephone lines, LAN or WAN links (e.g., T1, T3, 56kb, X.25), broadband connections (ISDN, Frame Relay, ATM), wireless connections and the like. The connections can be established using a variety of communication protocols (e.g., HTTP(S), TCP/IP, SSL, IPX, SPX, NetBIOS, Ethernet, RS232, direct asynchronous connections, a proprietary protocol and the like). In one embodiment, the server 108 and the client 112 encrypt all communication when communicating with each other.

[0031] The server node 108 can be any computing device capable of providing the services requested by the client node 112. Particularly, this includes authenticating a user at the client node 112 using biometric data, as described in more detail below. The server node 108 may include a network interface module 124, an authentication module 128, an augmentor module 132 and a storage module 135. The storage module 135 (which may be, for example, persistent memory, one or more hard disks, optical drives and the like) can include a template 136, in which a reference set of biometric data is stored. The server node 108 can also include one or more optional modules that add additional features for the collection of biometric data and are used in path 138, i.e., between the network interface module 124 and the authentication module 128. For example, the server 108 can include a normalizer module 142, a filter module 144 and/or an extractor module 146. The modules discussed throughout the specification are implemented as a software program and/or a hardware device (e.g., ASIC, FPGA, processor, memory, storage and the like). In one embodiment, one or more of the optional modules 142,

144 and/or 146 may be included on the client 112 instead of or in addition to the server 108. Placing the one or more of the optional modules 142, 144 and/or 146 on the client 112 distributes the processing task and lowers needed bandwidth on the network 116.

[0032] For clarity, FIG. 1 depicts server node 108 as a single server. It is to be understood, however, that the server node 108 can also be implemented, for example, distributed on portions of several (i.e., more than two) servers. The client node 112 can be any computing device (e.g., a personal computer, set top box, wireless mobile phone, handheld device, personal digital assistant, kiosk, etc) used to provide a user interface to access the server 108. The client node 112 receives biometric data from a biometric input device 160 (e.g., a fingerprint scanner, a retina scanner, a thermal imager, a skin spectrometer, a voice print analyzer, a digital camera and the like).

[0033] To use the system 100, a user 170, also referred to as a subscriber, registers that user's 170 biometric data with the system 100. In the illustrated embodiment, the client 112 receives biometric data from the biometric input device 160. The biometric data can include, for example, data associated with the individual's fingerprint(s), facial characteristics, voice and the like. The system 100 stores a set of biometric data associated with the user 170 in the storage module 135. In one embodiment, the biometric data is stored using an alias (e.g., a unique identifier with no personal or other type of information that can identify an individual), so that if the security of the storage module 135 is compromised, the biometric data cannot be associated with a particular individual.

[0034] In general overview, when the user 170 requests a service over the network 116 that requires authentication, the client device 112 receives a candidate set of biometric data from the biometric input device 160 and transmits it to the server node 108. The network interface module 124 receives the candidate set of biometric data and transmits it to the authentication module 128. The authentication module 128 retrieves a reference set of biometric data

associated with the user 170 from the storage module 135. If the candidate set of biometric data sufficiently matches the reference set of biometric data, the authentication module 128 authenticates the user as the registered individual.

[0035] To authenticate, the authentication module 128 and/or the optional modules 142, 144 and/or 146 process the received candidate set of biometric data to extract the unique features that distinguish one set of biometric data (e.g., fingerprint) from another. For example, the normalizer module 142 normalizes the biometric data into a format used by the authentication module 128 and stored in the storage module 135. The normalization can include, for example, a translation algorithm, a transformation algorithm and the like. The normalization allows the biometrics data to be converted into a standard image suitable for subsequent processing and preferably includes geometric processing to adjust for size differences between sensors, orientation adjustments to invert or rotate images, density adjustments to correct for number of gray levels/dynamic range and sampling adjustments to account for different sensor resolutions. This allows the client device 112 to interface with different types of biometric input devices 160 (e.g., fingerprint readers produced by different manufacturers and having diverse capture resolutions or characteristics) without the need to re-register the user 170 or change the format of the biometric data in the storage module 135.

[0036] The filter module 144 filters the received candidate set of biometric data. The filtering can include standard filtering algorithms for correcting blurring of the image, for removing random noise in the image and the like. For example, all captured scans can be checked for partial or blurred prints that exhibit greater than expected amount of change between consecutive frames as well as contrast. Images that exhibit excessive blur can be rejected. Contrast issues can be resolved by asking the user to press down to make better contact with the sensor. Image processing software may be used to enhance the quality of the image and involve signal averaging, noise filtering, ridge/valley enhancement as well as gray scale equalization. The

filtering can also include filtering algorithms needed because of the type of the biometric device 160 or the type of user features the biometric device 160 uses. The filtering can also include filtering algorithms based on the type of image (e.g., grainy, wet, fine grain and the like), the finger type and/or personal biometric characteristics (e.g., sex, age and the like). In an embodiment where the filter module 144 is implemented on the client 112, the filter module 114 operates in conjunction with the biometric input device 116 to perform blur removal, finger detection and time based enhancements. For example, two or more scans may be taken to ensure the user 170 has placed a stable finger (not moving) on the sensor. A difference is then taken between subsequent scans to ensure consistency between the two scans. With noisy sensors, the filter module 144 may integrate consecutive images to reduce the noise level in the captured image.

[0037] The extractor module 146 extracts the geometric data representing biometric features and/or minutiae from the candidate set of biometric data. In an embodiment where the extractor module 146 is implemented on the client 112, the extractor module 146 transmits the results to the authentication module 128 using the network 116. Biometric data, for example in the case of fingerprints, can be divided into global features that are spatial in nature and local features that represent details captured in specific locations. The geometric data can include, for example in the case of fingerprints, the locations (e.g., x, y coordinates) of the features, the type of feature (e.g., ridge ending, bifurcation and the like), the angular data of the features, the slope of the ridge, the neighborhood ridge counts and/or the like. Once the geometric data is processed, the authentication module 128 compares the data of the reference set of biometric data stored in the storage module 135 with the candidate set of biometric data to produce a goodness of fit or confidence of match by examining the local features on a minutia by minutia basis. To calculate the goodness of fit, the authentication module 128 determines the best spatial alignment between the location of minutiae points within the reference set of biometric data and corresponding

minutiae points within the candidate set of biometric data. Determining the best spatial alignment involves, for example, finding the rotation angle that produces the greatest number of matching points. Matching can be a relative term, meaning the points are close to each other within some predefined distance. The determining process preferably accommodates both spatial and rotational displacement between the reference set of biometric data and the candidate set of biometric data. This may be accomplished, for example, using a spatial correlation algorithm in which the features of the candidate set of biometric data are translated and rotated about a test alignment point and then compared against the features in the reference set. Different alignment points and rotation angles are tested to determine the lowest difference between the candidate and reference feature set. Once the differences between the local features at each of the matching minutiae points are minimized, the authentication module 128 sums the goodness of fit.

[0038] The authentication module 128 determines the sufficiency of the match by statistically analyzing the goodness of fit for local features at each of the matching minutiae points and determining whether the probability that they come from the same individual is above a certain predetermined threshold. In one embodiment, an administrator of the system 100 sets the predetermined threshold. The predetermined threshold determines both the false acceptance rate (i.e., the probability that the authentication module 128 will incorrectly authenticate a user) and the false rejection rate (i.e., the probability that the authentication module 128 will incorrectly reject the user when that user is in fact the registered individual). The administrator sets the predetermined threshold such that the false acceptance rate and the false rejection rate are both acceptable to the users of the system 100.

[0039] In addition, with the sufficient match, the authentication module 128 transmits the candidate set of the biometric data to the augmentor module 132, which in turn modifies the current reference set of biometric data (e.g., template 136) using the candidate set of biometric

data. The modification can include several different aspects of the reference biometric data. For example, one aspect is the spatial aspect (e.g., the associated data representing geometric features) of the reference set of the biometric data. Another aspect is the statistical aspect (e.g., the weighting and/or confidence level of features) of the reference set of the biometric data.

[0040] FIG. 2 illustrates an exemplary embodiment of a supertemplate 200 used to authenticate a user in accordance with the invention. The supertemplate 200 represents a set of biometric data corresponding to a complete set of biometric data. For example, in a fingerprint system, the supertemplate 200 represents the complete set of biometric data for one digit. Superimposed on the supertemplate 200 are a first set of biometric data 205, a second set of biometric data 210, a third set biometric data 215 and a fourth set of biometric data 220. As illustrated, the sets of biometric data 205, 210, 215 and 220 are smaller in size than the supertemplate 200. In one embodiment, the sets of biometric data 205, 210, 215 and 220 represent templates 136. The supertemplate 200 can comprise one or more templates 136. The size of the sets of biometric data 205, 210, 215 and 220 are based on the biometric input device 160. For example, the size of the scanner, the size of the local memory and the like. It is noteworthy that even if the scanner is large enough to cover the entire finger the supertemplate 200 can accumulate additional information from multiple templates 205, 210, 215 and 220 to generate more accurate statistics for the features.

[0041] For an illustrative example of the modifying process, a reference set of biometric data is the supertemplate 200 and a candidate set of biometric data for a first authentication request is equivalent to the biometric data represented in the first set of biometric data 205. As described above, upon a sufficient match, the augmentor module 132 modifies the supertemplate 200 using the candidate set of biometric data. For the sufficient match, the authentication module 128 matches features of the candidate set of biometric data with features of the reference data

included in the supertemplate 200. The augmentor module 132 aligns those matched features to determine how the candidate set of biometric data fits into the supertemplate 200.

[0042] When the augmentor module 132 determines the alignment, the augmentor 132 modifies the template 200 using the candidate set of biometric data. The results are that in this illustrative example, the area indicated as the first set of biometric data 205 is modified with the candidate set of biometric data. In one embodiment, the augmentor module 132 modifies by replacing the features in the existing reference biometric data in the area indicated as the first set of biometric data 205 with the candidate set of biometric data received by the client 112. In this way, the system accommodates feature changes that occur over time (e.g., due to aging of the user). In another embodiment, the augmentor module 132 augments the existing reference biometric data by adding in those features of the candidate set of biometric data that are not matched and/or not presently included in the reference set of biometric data. This allows the system 100 to build a fuller biometric representation than would be possible with, for example, a single scan by the biometric input device 160. Augmented in this fashion, the supertemplate 200 can evaluate scans covering different portions of, for example, the user's fingerprint, increasing the system's tolerance for variation without sacrificing accuracy (i.e., the number of feature points matched).

[0043] Continuing with the illustrative example of the modifying process, a candidate set of biometric data for a second authentication request is equivalent to the biometric data represented in the second set of biometric data 210. As described above, upon a sufficient match, the augmentor module 132 aligns those matched features to determine how the candidate set of biometric data fits into the supertemplate 200. Once the augmentor module 132 determines the alignment, the augmentor 132 modifies the template 200 using the candidate set of biometric data. The results are that in this illustrative example, the area indicated as the second set of biometric data 210 is modified with the candidate set of biometric data. Similarly in subsequent

authentication requests, the augmentor module 132 modifies the areas indicated as the third and fourth sets of biometric data, 220, 225 respectively.

[0044] As described above, in addition to the modification of features, the augmentor module 132 also modifies the statistical parameters of the reference set of biometric data. Each time features in a candidate set of biometric data match the features of the reference set biometric data, the augmentor module 132 increases the weighting and/or confidence level of those matched features. The area 230, indicated by shading, represents the overlap of all of the sets of biometric data (205, 210, 215 and 225). The weighting and/or confidence level of the matched features in this area 230 is the highest, as it has been reinforced by the redundant presence of the matched features in each of the four received candidate sets of biometric data. The closeness of the match can also affect the value of the weighting and/or confidence level. For example those features that directly overlap with two candidate sets of biometric data have a higher weighting and/or confidence level than those features that are close, but have some small distance between them.

[0045] In broad overview, FIG. 3 illustrates another embodiment of system 100' to authenticate a user using augmented biometric data in accordance with the invention. The server node 108' of the system 100' includes a network interface module 124', an authentication module 128', a storage module 135, having a template 136' stored therein, and a modification module 320. The client node 112' of the system includes a client comparator module 330.

[0046] To use the system 100', the user 170 registers that user's 170 biometric data with the system 100', as described above. For authenticating, the server 108' and client 112' use a challenge-response protocol that does not transmit a full set of biometric data across the network 116. This challenge-response protocol modifies a portion of the set of biometric data sent across the network 116 so that if intercepted by someone, it is not usable in its modified state. FIG. 4 depicts a supertemplate 200' that the system 100' employs to implement the challenge-response

protocol. The supertemplate 200' includes a challenge template 405 that represents a set of biometric data. In one embodiment, the challenge template 405 is equivalent in area to the template 136'. As described above, the template 136' varies in size and is at least a portion of the supertemplate 200'. The challenge template 405 includes a first portion 410 and a second portion 420. As illustrated, the first portion 410 and the second portion 420 include random feature data, as described in more detail below.

[0047] FIG. 5 illustrates an embodiment of a process 500 to authenticate a user 170 using the challenge-response protocol, a system 100' as depicted, for example, in FIG. 3 and a challenge template 405 as depicted, for example, in FIG. 4. In operation, the client 112', in response to a user 170 action, generates (step 505) a request. The request can be an authentication request directly from the client 112 to authenticate the user 170. The request can also be a service request for a certain service (e.g., execution of an application program, access to a financial or medical database, access to an electronic vault with which the user 170 is associated, download of data and/or an application program, and the like) provided by a server on the network (e.g., 108' or a different application server). In that case, the server providing the requested service transmits a request for authentication to the authentication module 128'.

[0048] In response to the authentication request, the modification module 320 copies (step 510) the template 136' of the reference biometric data associated with the user 170. The modification module 320 generates (step 515) modification data and uses this modification data to modify (step 520) the copy of the template to generate a challenge template 405. For an illustrative example, the modification module 320 copies (step 510) at least a portion of the geometric data contained within the reference template 136', for example, the x, y coordinates of the features. To generate the modification data, the modification module 320 generates random x, y locations and thereby generates random modified features at these locations in the challenge template 405. In another embodiment, the modification data is not random but generated by an algorithm that

is dependent on the biometric data, thus creating different modification data for different users. The modification module 320 modifies (step 520) the copy of the reference template (i.e., challenge template 405) by inserting the modification data into the challenge template 405, for example at the random x, y locations. The modification module 320 can also create the modification data used for the challenge template 405 by combining features from other users or other fingers to create a composite that is similar to real data because the modification data is based on real biometric data. For example, the modification module 320 can create the composite modification data from other users and then align the end points when inserting this composite modification data in portion 410, so it looks like real data, but would not be matchable without knowing which areas were false.

[0049] For clarity and illustration only, the modification data for this particular request of the illustrated process 500 fall within the first and second portions, 410 and 420 respectively, of the challenge template 405. Of course, if the modification data were random, then the modified x, y coordinates would be distributed randomly throughout the challenge template area. In another embodiment, the modification module 320 can insert random noise in portions of the challenge template 405, for example, in the first and second portions, 410 and 420 respectively. Once the modification module 320 generates the challenge template 405, the server 108' transmits the challenge template 405 to the client 112. As stated above, with random data inserted in the first location 410 and the second location 420, even if the challenge template 405 is copied by an eavesdropper, the challenge template 405 is not usable because the biometric data in those locations will not match reference biometric data (e.g., reference template 136') stored for that user in biometric authentication systems.

[0050] The comparator module 330 of the client 112' receives (step 530) a set of candidate biometric data from the biometric input device 160. The comparator module 330 compares (step 535) the candidate set of biometric data with the received challenge template 405. The

comparator module 330, for example, can spatially align the candidate set of biometric data with the challenge template 405, maximizing the number of matching features, and then calculate a degree of overlapping (i.e., matching) of the features at various x, y coordinates. The comparator module 330 generates (step 540) a response vector, for example, listing the x, y coordinates and the degree of matching. Another format can include the actual candidate features found in all matching areas. Other formats for the response vector include listing the x, y coordinates that are above (or below) a certain threshold, listing the x, y coordinates with no matching features, generating a hash code using the challenge template 405 and the candidate set of biometric data, and the like. The client 112' transmits the response vector back to the server 108'. The transmitted response vector does not include a full set of biometric data, so it is not usable if someone intercepts it.

[0051] The authentication module 128' receives the response vector and compares (step 550) the response vector with the modification data. The authentication module 128' determines (step 555) if the comparison between the response vector and the modification data indicates that there is a sufficient match, or in other words, that the user 170 is, to a statistical degree of certainty, the registered individual. If the authentication module 128' determines that the comparison indicates there is not a sufficient match, the authentication module 128' denies (step 560) the user 1780 as the registered individual. If the authentication module 128' determines that the comparison indicates there is a sufficient match, the authentication module 128' authenticates (step 565) the user 1780 as the registered individual.

[0052] Ideally, when the user 170 is the registered individual, the mismatches identified in the response vector coordinate with the modification data in the first location 410 and the second location 420, while the features outside of these locations match to a high degree of probability. Deviations from this ideal can be caused by noise introduced by the biometric input device 160, different sizes of the candidate set of biometric data and the challenge template 405, rotation

and/or motion of the user's finger while scanning, and the like. As described above, the authentication module 128' statistically analyzes the mismatches, accounting for those due to the modification data, and determines to a statistical certainty whether the matches indicate that the user 170 is the registered individual.

Equivalents

[0053] The invention can be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The foregoing embodiments are therefore to be considered in all respects illustrative rather than limiting on the invention described herein. Scope of the invention is thus indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

CLAIMS

What is claimed is:

1. A method for authentication using biometrics, the method comprising:

receiving an authentication request requesting authentication of a user;

receiving a first set of biometric data from the user;

comparing the first set of biometric data with a second set of biometric data in storage; and

if the second set of biometric data sufficiently matches the first set of biometric data, modifying the second set of biometric data in storage based at least in part on the first set of biometric data.

2. The method of claim 1 wherein the modifying step comprises, if the second set of biometric data sufficiently matches the first set of biometric data, replacing the second set of biometric data in storage with the first set of biometric data.

3. The method of claim 1 wherein the modifying step further comprises:

identifying one or more features in the first set of biometric data;

matching at least a portion of the one or more features in the second set of biometric data; and

augmenting the second set of biometric data with the first set of biometric data based at least in part on the matched features.

4. The method of claim 3 wherein the augmenting step further comprises augmenting the second set of biometric data with features from the first set of biometric data not presently included in the second set of biometric data.

5. The method of claim 3 wherein the augmenting step further comprises augmenting statistical data associated with the second set of biometric data based at least in part on the first set of biometric data.

6. The method of claim 5 wherein the step of augmenting statistical data further comprises increasing the weighting of the matched features.

7. The method of claim 1 further comprising normalizing the first set of biometric data.

8. The method of claim 1 further comprising filtering the first set of biometric data.

9. The method of claim 1 further comprising extracting from the first set of biometric data identifying features.

10. The method of claim 1 wherein the second set of biometric data is stored in a supertemplate.

11. A system for authentication using biometrics, the system comprising:

a network interface module configured to receive an authentication request requesting authentication of a user and to receive a first set of biometric data from the user;

a storage module configured to store a second set of biometric data;

an authentication module configured to compare the first set of biometric data with the second set of biometric data in storage; and

an augmentor module configured to modify the second set of biometric data in storage based at least in part on the first set of biometric data if the second set of biometric data sufficiently matches the first set of biometric data.

12. The system of claim 11 wherein the augmentor module is further configured to replace the second set of biometric data in storage with the first set of biometric data if the second set of biometric data sufficiently matches the first set of biometric data.

13. The system of claim 11 wherein the augmentor module is further configured i) to identify one or more features in the first set of biometric data, ii) to match at least a portion of the one or more features in the second set of biometric data and iii) to augment the second set of biometric data with the first set of biometric data based at least in part on the matched features.

14. The system of claim 13 wherein the augmentor module is further configured to augment the second set of biometric data with features from the first set of biometric data not presently included in the second set of biometric data.

15. The system of claim 13 wherein the augmentor module is further configured to augment statistical data associated with the second set of biometric data based at least in part on the first set of biometric data.

16. The system of claim 15 wherein the augmentor module is further configured to increase the weighting of the matched features.

17. The system of claim 11 further comprising a normalizer module configured to normalize the first set of biometric data.

18. The system of claim 11 further comprising a filter module configured to filter the first set of biometric data.

19. The system of claim 11 further comprising an extractor module configured to extract from the first set of biometric data identifying features.

20. The system of claim 11 wherein the second set of biometric data is stored in a supertemplate.

21. An article of manufacture having computer-readable program portions embodied therein for authentication using biometrics, the article comprising:

a computer-readable program portion for receiving an authentication request requesting authentication of a user;

a computer-readable program portion for receiving a first set of biometric data from the user;

a computer-readable program portion for comparing the first set of biometric data with a second set of biometric data in storage; and

a computer-readable program portion for modifying the second set of biometric data in storage based at least in part on the first set of biometric data if the second set of biometric data sufficiently matches the first set of biometric data.

22. The article of claim 21 wherein the modifying step further comprises:

a computer-readable program portion for identifying one or more features in the first set of biometric data;

a computer-readable program portion for matching at least a portion of the one or more features in the second set of biometric data; and

a computer-readable program portion for augmenting the second set of biometric data with the first set of biometric data based at least in part on the matched features.

23. A method for authentication using biometrics, the method comprising:

providing a reference template with a reference set of biometric data associated with an individual;

receiving an authentication request associated with a user;

generating a copy of the reference template;

modifying the copy of the reference template with modification data to generate a challenge template;

transmitting the challenge template;

receiving a response vector based at least in part on the challenge template and a candidate set of biometric data; and

authenticating the user as the individual associated with the reference set of biometric data based at least in part on the response vector and the modification data.

24. The method of claim 23 further comprising:

receiving the candidate set of biometric data associated with the user; and

comparing the candidate set of biometric data with the challenge template thereby generating the response vector.

25. The method of claim 24 wherein the comparing step further comprises:

determining features in the candidate set of biometric data that match; and

determining features in the candidate set of biometric data that do not match.

26. The method of claim 25 wherein the authenticating step further comprises authenticating the user as the individual associated with the reference set of biometric data if the matched features is not less than a predetermined threshold and the mismatched features sufficiently matches the modification data.

27. The method of claim 23 further comprising registering the individual by generating the reference template with the reference set of biometric data from the individual.

28. The method of claim 23 wherein the authenticating step further comprises authenticating the user as the individual associated with the reference set of biometric data if at least a portion of the data represented by the response vector sufficiently matches the modification data.

29. The method of claim 23 wherein the modification data contains random data.

30. The method of claim 23 wherein the response vector is a hash result.

31. The method of claim 23 wherein the reference template is a portion of a supertemplate.

32. A system for authentication using biometrics, the system comprising a server including:

a reference template having a reference set of biometric data associated with an individual;

a modification module configured to generate a copy of the reference template and modify the copy of the reference template with modification data to generate a challenge template; and

an authentication module configured i) to receive a response vector based at least in part on the challenge template and a candidate set of biometric data and ii) to

authenticate a user as the registered individual in response to the response vector and the modification data.

33. The system of claim 32 wherein the modification data contains random data.

34. The system of claim 32 wherein the response vector is a hash result.

35. The system of claim 32 wherein the template is a portion of a supertemplate.

36. The system of claim 32 further comprising:

a client in communication with the server, the client including:

a comparator module configured to compare the candidate set of biometric data, associated with the user, with the challenge template thereby generating the response vector.

37. The system of claim 36 wherein the comparator module is further configured i) to determine features in the candidate set of biometric data that match and ii) to determine features in the candidate set of biometric data that do not match.

38. The system of claim 37 wherein the authentication module is further configured to authenticate the user as the individual associated with the reference set of biometric data if the matched features is not less than a predetermined threshold and the mismatched features sufficiently matches the modification data.

39. The system of claim 32 further comprising a registration module configured to generate the reference template with the reference set of biometric data from the individual.

40. The system of claim 32 wherein the authentication module is further configured to authenticate the user as the individual associated with the reference set of biometric data if at least a portion of the data represented by the response vector sufficiently matches the modification data.

41. An article of manufacture having computer-readable program portions embodied therein for authentication using biometrics, the article comprising:

a computer-readable program portion for providing a reference template with a reference set of biometric data associated with an individual;

a computer-readable program portion for receiving an authentication request associated with a user;

a computer-readable program portion for generating a copy of the reference template;

a computer-readable program portion for modifying the copy of the reference template with modification data to generate a challenge template;

a computer-readable program portion for transmitting the challenge template;

a computer-readable program portion for receiving a response vector based at least in part on the challenge template and a candidate set of biometric data; and

a computer-readable program portion for authenticating the user as the registered individual based at least in part on the response vector and the modification data.

42. The article of claim 41 further comprising

a computer-readable program portion for receiving the candidate set of biometric data associated with the user; and

a computer-readable program portion for comparing the candidate set of biometric data with the challenge template thereby generating the response vector.

43. The article of claim 42 further comprising a computer-readable program portion for registering the individual by generating the reference template with the reference set of biometric data from the individual.

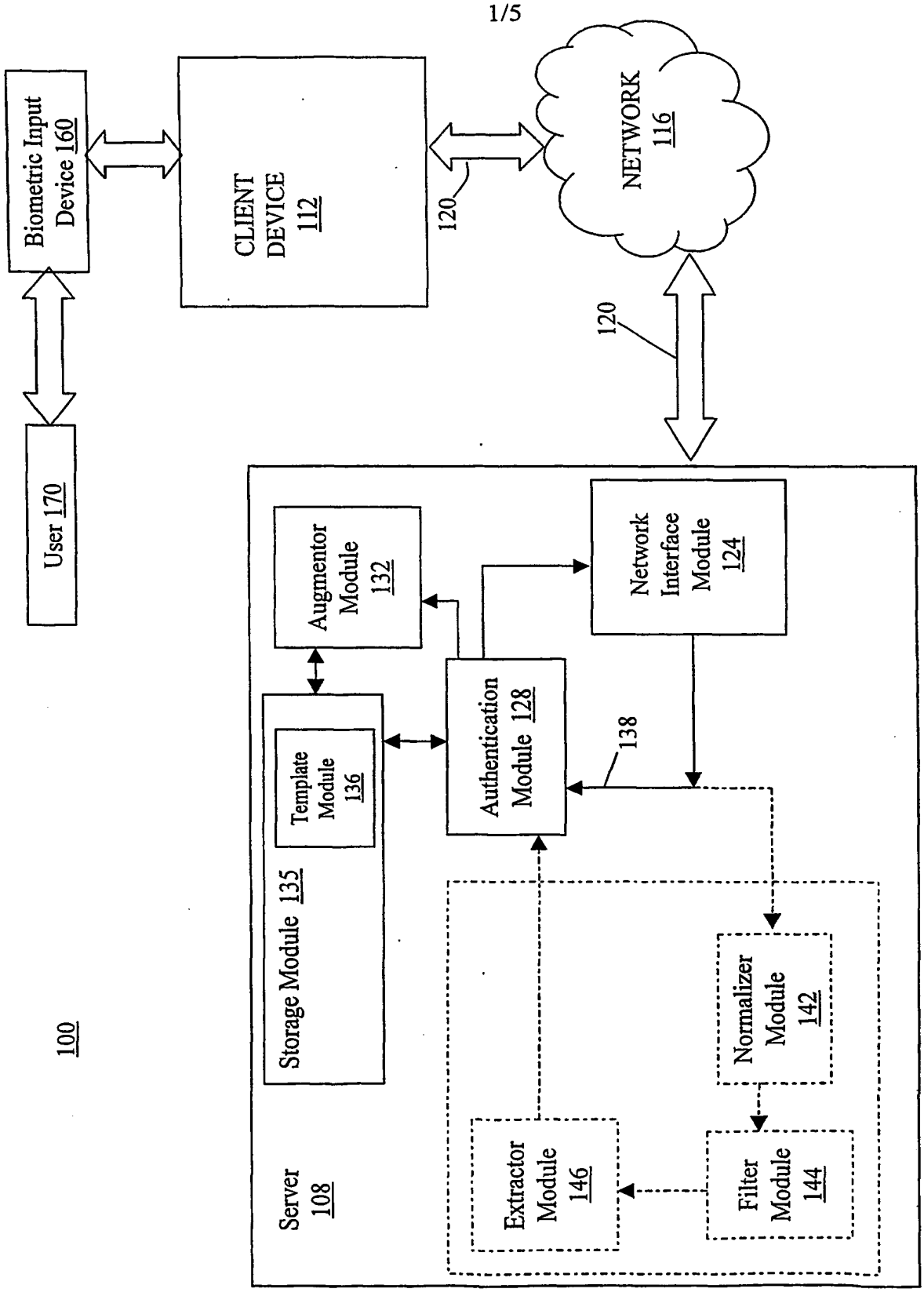

100
Biometric Input Device 160
User 170
CLIENT DEVICE 112
120
NETWORK 116
120
Server 108
Storage Module 135
Template Module 136
Augmentor Module 132
Authentication Module 128
138
Network Interface Module 124
Extractor Module 146
Normalizer Module 142
Filter Module 144

FIG. 1

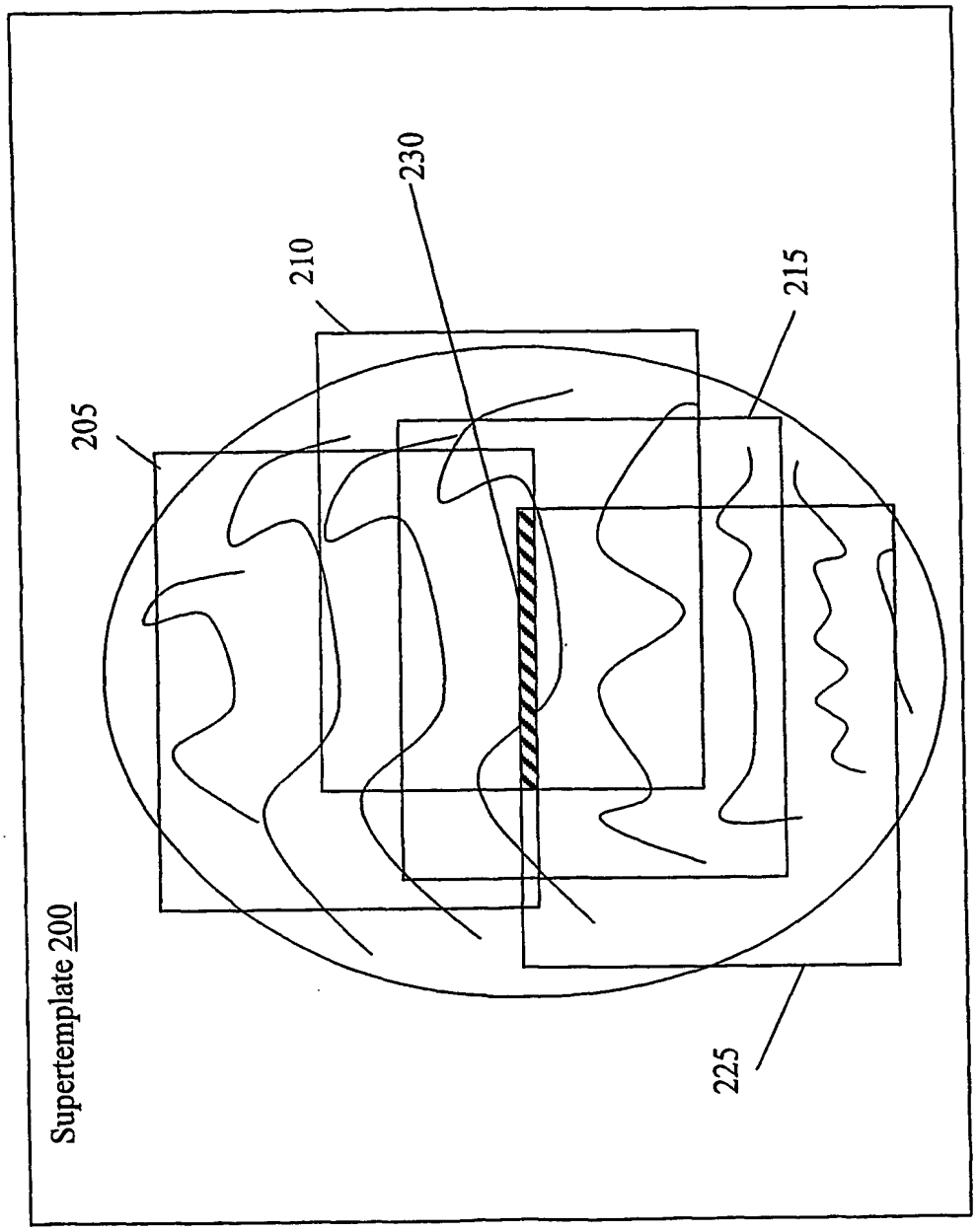


FIG. 2

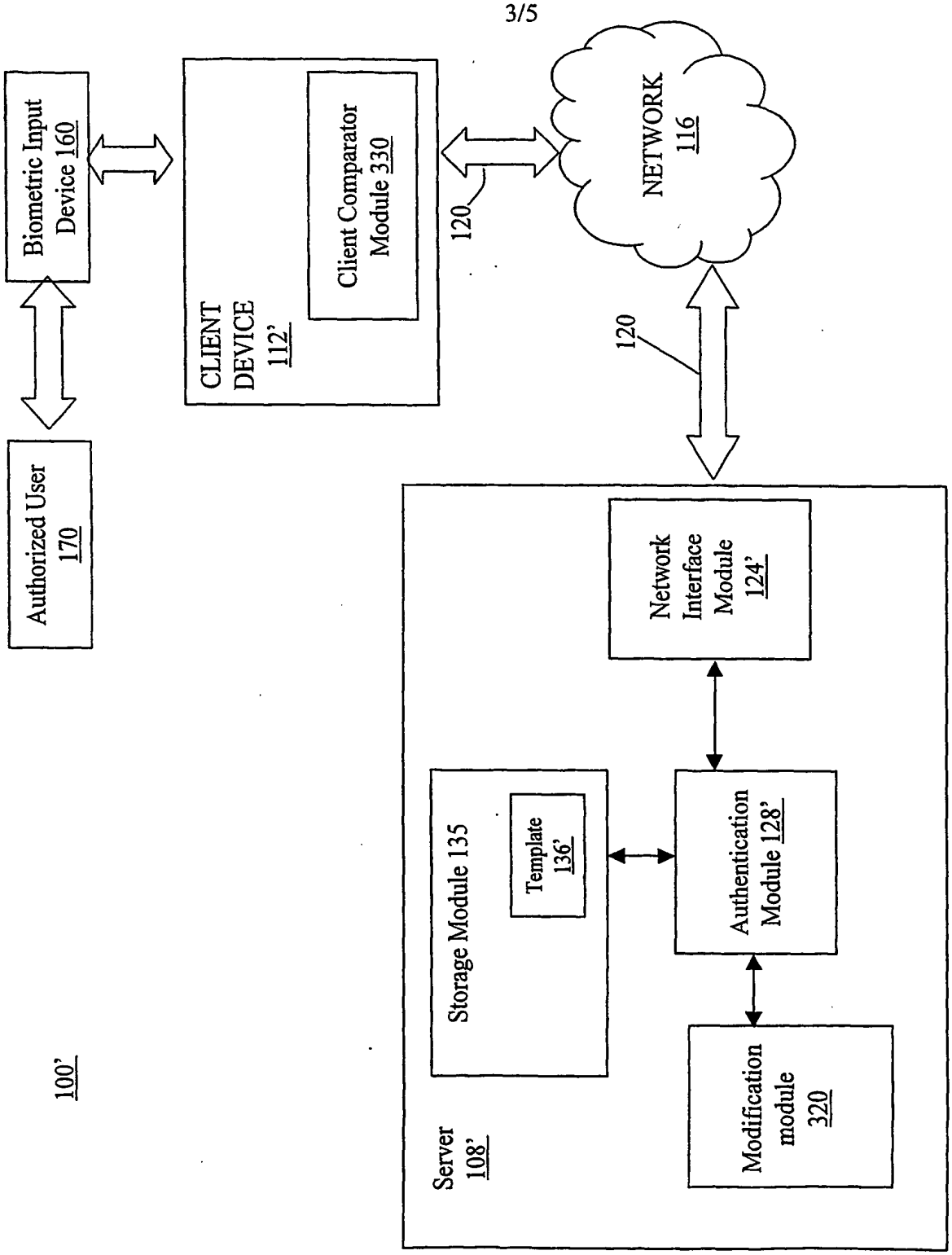

100'
Biometric Input Device 160
Authorized User 170
CLIENT DEVICE 112'
Client Comparator Module 330
120
NETWORK 116
120
Server 108'
Network Interface Module 124'
Storage Module 135
Template 136'
Authentication Module 128'
Modification module 320

FIG. 3

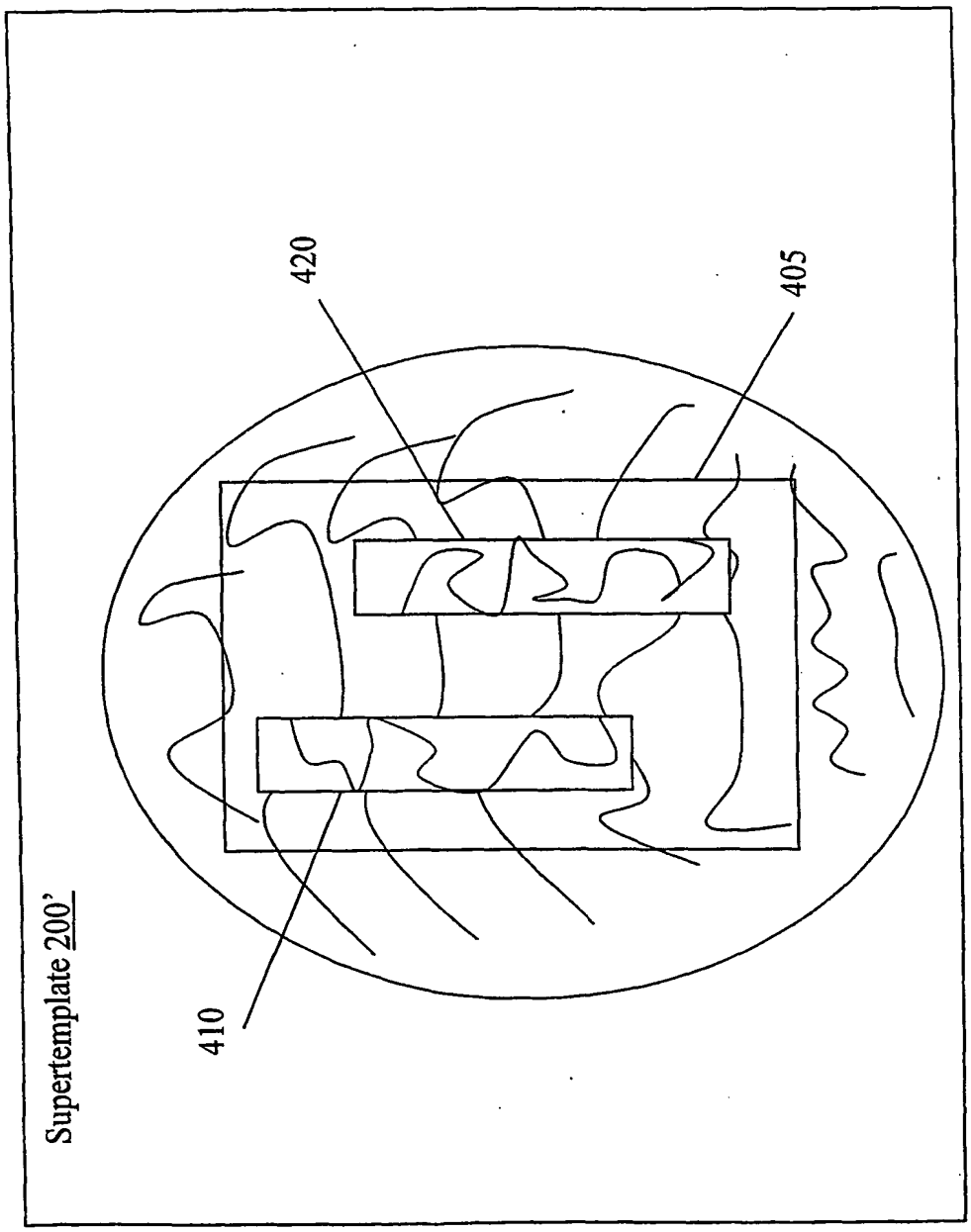


FIG. 4

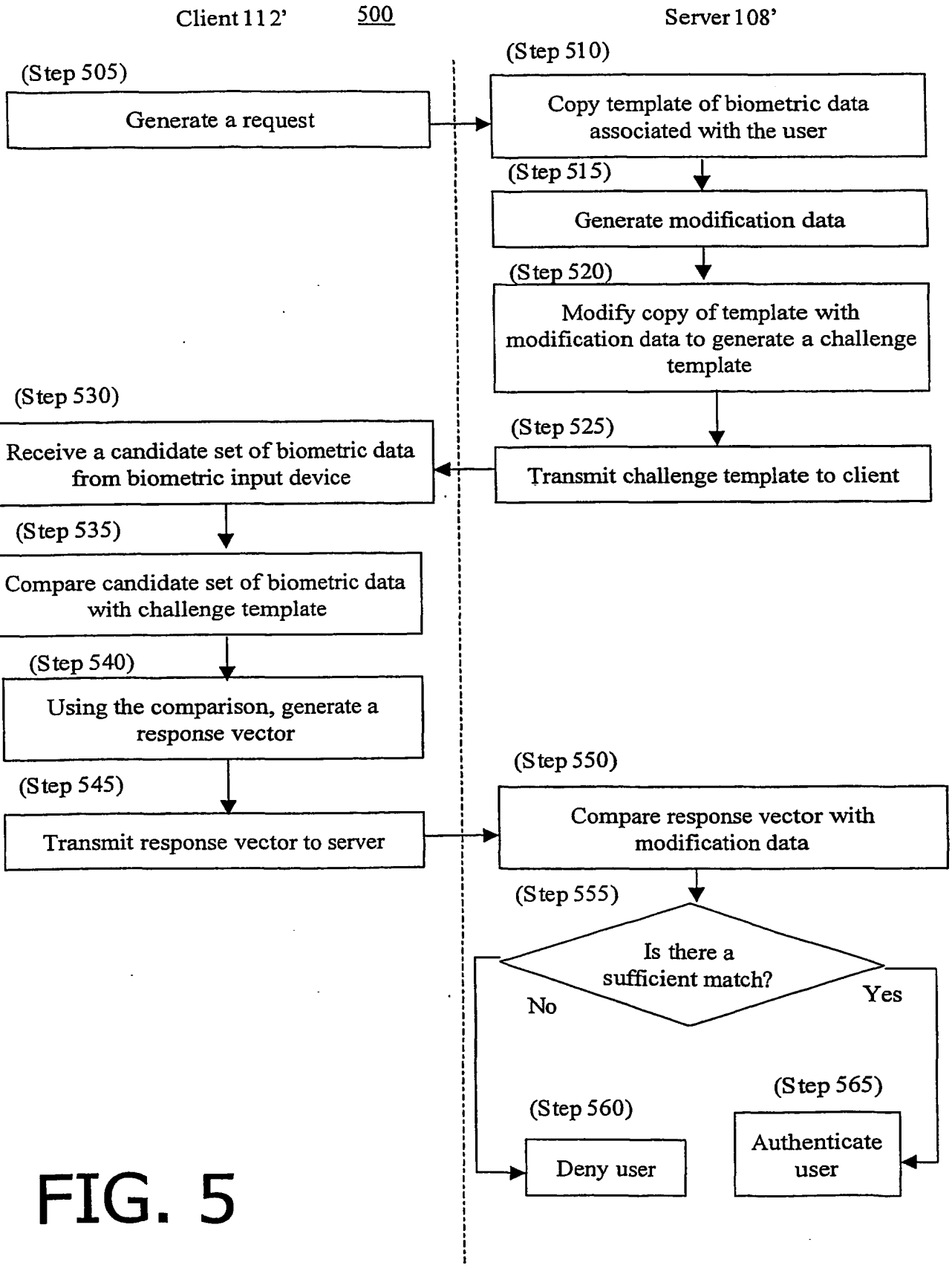

Client 112'
500
Server 108'
(Step 505)
Generate a request
(Step 510)
Copy template of biometric data associated with the user
(Step 515)
Generate modification data
(Step 520)
Modify copy of template with modification data to generate a challenge template
(Step 525)
Transmit challenge template to client
(Step 530)
Receive a candidate set of biometric data from biometric input device
(Step 535)
Compare candidate set of biometric data with challenge template
(Step 540)
Using the comparison, generate a response vector
(Step 545)
Transmit response vector to server
(Step 550)
Compare response vector with modification data
(Step 555)
Is there a sufficient match?
No
Yes
(Step 560)
Deny user
(Step 565)
Authenticate user

FIG. 5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2002 (28.11.2002)

PCT

(10) International Publication Number
WO 2002/095552 A3

(51) International Patent Classification[7]: G06F 1/00, 21/00, H04L 29/06, G07C 9/00

(21) International Application Number: PCT/US2002/015466

(22) International Filing Date: 17 May 2002 (17.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/291,900 18 May 2001 (18.05.2001) US

(71) Applicant: IMPRIVATA, INC. [US/US]; 10 Maguire Road, Lexington, MA 02421 (US).

(72) Inventor: TING, David, M., T.; 27 Woodland Road, Sudbury, MA 01776 (US).

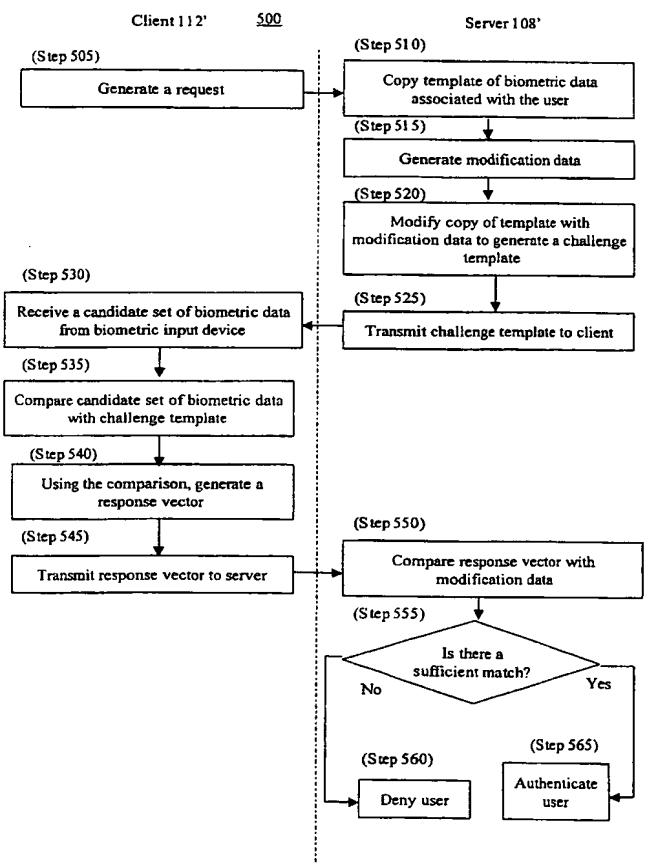
(74) Agent: MIRANDA, David, G.; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: AUTHENTICATION WITH VARIABLE BIOMETRIC TEMPLATES



(57) Abstract: The invention relates to systems and methods for using a template in the authentication process using biometric data. In one embodiment, a module modifies a template of the reference set of biometric data with the candidate set of biometric data when the user is authenticated. In another embodiment, a module modifies a copy of the template of the reference biometric data with modification data thereby creating a challenge template. The client compares the challenge template to a candidate set of biometric data thereby creating a response vector. A module authenticates the user based on the response vector and the modification data.

WO 2002/095552 A3

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
29 April 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/15466

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F21/00 H04L29/06 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 857 028 A (FRIELING EDWARD) 5 January 1999 (1999-01-05) abstract column 3, line 22 - column 5, line 20 column 8, line 51 - column 9, line 44; figure 6 -----	1-4, 11-14, 21,22
X	WO 98/16906 A (KOMMER ROBERT VAN ;TELECOM PTT (CH); MOSER THOMAS (CH)) 23 April 1998 (1998-04-23) page 3, line 19 - last line page 6, paragraph 2 - page 7, paragraph 2; figures 1,4 page 9, paragraph 2 ----- -/--	1-4, 11-14, 21,22

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2003	15.03.2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Beker, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat[redacted] Application No
PCT/US 02/15466

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 2001/036299 A1 (SENIOR ANDREW WILLIAM) 1 November 2001 (2001-11-01) paragraphs [0051] - [0064]; figure 4	1-4, 11-14, 21,22

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 02/15466

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this International application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-4, 11-14, 21, 22

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-4,11-14,21-22

   Method, system and article of manufacture employing authentification based on the comparison of first biometric data received from a user with a stored second set of biometric data which are updated on the bases of the first set of biometric data

   ---

2. claims: 5-6,9,15-16,19

   Method, system and article of manufacture employing authentification based on the comparison of first biometric data received from a user with a stored second set of biometric data which are updated on the bases of the first set of biometric data in which statistical data associated with the second set of biometric data are modified in accordance with the first set of biometric data.

   ---

3. claims: 7,17

   Method, system and article of manufacture employing authentification based on the comparison of first biometric data received from a user with a stored second set of biometric data which are updated on the bases of the first set of biometric data in which the first set of biometric data is normalised

   ---

4. claims: 8,18

   Method, system and article of manufacture employing authentification based on the comparison of first biometric data received from a user with a stored second set of biometric data which are updated on the bases of the first set of biometric data in which the first biometric data are filtered

   ---

5. claims: 10,20

   Method, system and article of manufacture employing authentification based on the comparison of first biometric data received from a user with a stored second set of biometric data which are updated on the bases of the first set of biometric data in which the second set of biometric data is stored in a supertemplate

   ---

6. claims: 23-43

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Method, system and article of manufacture employing biometric authentification in which a challange based on a modified reference template of biometric data is transmitted as a challange template and receiving a response vector based the difference of a candidate set of biometric data and said modified reference template

---

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 02/15466

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5857028 A	05-01-1999	NONE	
WO 9816906 A	23-04-1998	WO 9816906 A1	23-04-1998
		AT 227868 T	15-11-2002
		AU 7293096 A	11-05-1998
		CA 2267954 A1	23-04-1998
		CZ 9901257 A3	11-08-1999
		DE 69624848 D1	19-12-2002
		DE 69624848 T2	09-10-2003
		EP 0932885 A1	04-08-1999
		JP 2001503156 T	06-03-2001
		US 6556127 B1	29-04-2003
US 2001036299 A1	01-11-2001	NONE	

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.